PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2001-313635**

(43)Date of publication of application : **09.11.2001**

(51)Int.Cl. H04L 9/32
G06F 15/00

(21)Application number : **2000-130100**

(22)Date of filing : **28.04.2000**

(71)Applicant : **NIPPON TELEGR & TELEPH CORP <NTT>**

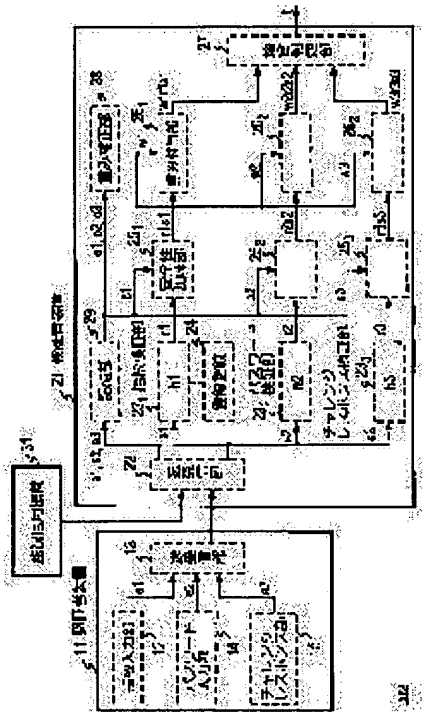
(72)Inventor : **OTSUKA HIROAKI**
MORITA HIKARI
GOHARA JUNICHI

(54) AUTHENTICATING METHOD AND ITS VERIFIER DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To cope with the deterioration of the security of authentication information.

SOLUTION: An authenticator device 11 sends each piece of authentication information e1, e2 and e3 of a fingerprint, a password and challenge response to a verifier device 21, and in the device 21, respective verifying parts 231, 232 and 233 verify the e1, e2 and e3, multiply these verification results r1, r2 and r3 by security indexes s1, s2 and s3 transmitted from a monitoring credit facilities 31 with respect to each type of the authentication information, further multiply the respective results r1, r2 and r3 by weighting coefficients w1, w2 and w3 with respect to each authentication information and defines w1r1s1+w2r2s2+w3r3s3=t as the total decision output. The parameter t is made to range between 0 and 1. When, for instance, the security of the password is deteriorated due to the elapse of time, the s2 is defined as small.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－313635
（P2001－313635A）
(43)公開日　平成13年11月9日(2001.11.9)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/32		Ｃ０６Ｆ　15/00	３３０Ｆ	５Ｂ０８５
Ｇ０６Ｆ　15/00	３３０		３３０Ｅ	５Ｊ１０４
		Ｈ０４Ｌ　9/00	６７３Ｄ	
			６７３Ａ	
			６７５Ｄ	

審査請求　未請求　請求項の数５　ＯＬ　（全６頁）

(21)出願番号　特願2000－130100(P2000－130100)

(22)出願日　平成12年４月28日(2000.4.28)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　大塚　浩昭
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　森田　光
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100066153
弁理士　草野　卓　（外１名）

最終頁に続く

(54)【発明の名称】　認証方法及びその検証者装置

(57)【要約】
【課題】　認証情報の安全性の低下に対応できる。
【解決手段】　認証者装置１１から指紋、パスワード及びチャレンジレスポンスの各認証情報ｅ１，ｅ２及びｅ３を検証者装置２１へ送り、装置２１ではｅ１，ｅ２，ｅ３に対しそれぞれの検証部23_1，23_2，23_3で検証し、これら検証結果ｒ１，ｒ２，ｒ３に対し、監視信用機関３１から送られた各種類の認証情報に対する安全指標ｓ１，ｓ２，ｓ３を乗算し、更にそれぞれに対し、各認証情報に対する重み付け係数ｗ１，ｗ２，ｗ３を乗算し、ｗ１ｒ１ｓ１＋ｗ２ｒ２ｓ２＋ｗ３ｒ３ｓ３＝ｔを総合判定出力とする。ｔは０～１の値をとるようにする。年月の経過により例えばパスワードに対する安全性が低下するとｓ２が小とされる。

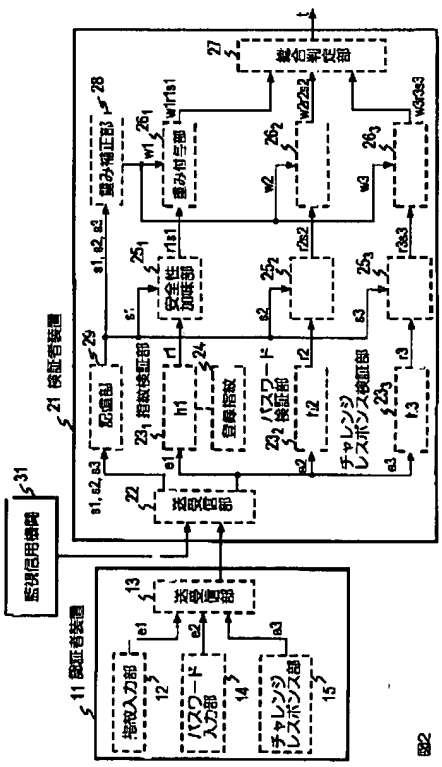


図2

する。

【0008】

【課題を解決するための手段】この発明によれば監視信用機関を導入し、監視信用機関により、各種認証情報の安全性に関し監視を行うことにより、安全性に関する指標を検証者装置へ報告し、検証者装置は、認証者装置から認証に関する情報を受けたとき、前記安全性に関する指標を加味した検証結果を出力する。検証者装置へ与えられる認証情報が複数の場合は、それぞれの検証結果に対し、安全性の指標を加味し、その安全性指標が加味された検証結果を総合した検証結果を出力する。つまり認証者装置から検証者装置へあたえられる各種認証情報をｅ１，ｅ２，…＝ｅｉ（ｉ＝１，２，…）とし、それぞれの認証情報による判定情報（検証結果）をｒ１，ｒ２，…＝ｒｉ＝ｈｉ（ｅｉ）（ｉ＝１，２，…）とし、ここでｈｉ（・）は各種認証情報ｅｉに対する個別の判定関数（検証関数）であり、ｒｉは０～１の間の値である。総合的な判定結果ｔは、ｆ（r_{x1}，r_{x2}，…，s_{x1}，s_{x2}，…）＝ｔであり、ｘ１，ｘ２，…＝ｘｉ（ｘｉ∈１，２，…）は認証者と検証者の間で決められた検証結果ｒｉに関する選定を示すとともに、ｓ１，ｓ２，…＝ｓｉ（ｉ＝１，２，…）は監視信用機関から与えられた安全指標であり、ｆ（・・）は判定情報（検証結果）と安全指標を入力として、総合的な判定結果を出す関数である。なおr_0＝０、s_0＝０とする。検証者はこの結果ｔを入手し、これを用いて認証者の有効無効を判断する。

【0009】なお安全指標の決定については監視信用機関において、各認証方法について手法に応じて認証情報の安全指標を決定して、公表し、新しい認証方法が現われ認証情報の安全指標を決定し、また先に述べたように例えばＤＥＳ暗号を用いる認証方法において、その安全性が低下すると、対応する認証情報の安全指標を低い値に変更する。パスワードを用いる認証方法の場合は、利用者が認証手続を行うことを実施し始めた時に、利用者が監視信用機関３１にそのことを登録すると、監視信用機関はその登録から例えば１年ごとのように年数が経過するごとに、そのパスワードの認証情報に対する安全指標を低下させ、それを利用者に通知することも考えられる。

【0010】

【発明の実施の形態】以下図面を用いてこの発明の実施例について詳しく説明する。ネットワーク上での利用者認証を例とした場合で、認証者装置１１と検証者装置２１と監視信用機関３１とで構成され、これらは通信手段４１で互いに接続することが可能である。

第一の実施例

まず、認証手段が１つしか存在しない例、すなわち認証者と検証者の間にて選定がｘ１＝１，ｘ２＝ｘ３＝…＝０と定められた場合について説明する。

【0011】認証者装置１１は指紋入力部１２により認証情報として認証者の指紋情報ｅ１を生成して送信部１３にて検証者装置２１に送るとする。この場合、検証者装置２１は受信部２２で受信した指紋情報ｅ１を検証部（指紋検証部）23_1に入力して、ｈ１（ｅ１）＝ｒ１を演算して認証者の指紋に関する判定情報ｒ１を得る。ｈ１（・）は、受信指紋情報ｅ１と記憶部２４に記憶されている登録指紋との一致性を判定する関数とする。ｒ１は０～１の範囲の値で、０ならば検証者装置２１に登録されている認証者の指紋と離れていて、１ならば検証者装置２１の記憶部２４に登録されている認証者の指紋にきわめて近いとする。この検証結果ｒ１に対し、安全指標ｓ１を安全性加味部25_1で加味し、例えばｒ１ｓ１とする。この実施例では認証情報が１つしかない場合であるからｔ＝ｒ１ｓ１として判定結果が出力され、このｔを用いて認証者の認証可否を判断する。ｓ１は、監視信用機関３１から送られ、受信部２２で受信され、記憶部２４に記憶されている指紋に関する安全指標である。

【0012】このように検証結果に対し、安全指標ｓ１が加味されているため、検証者は、その判定結果ｔに応じて対処する、つまり例えば認証に合格するとあるサービスを行う場合、そのサービスによっては厳しく本人性が要求される場合はｔが十分大でなければ、無効とするが、それ程本人性が厳しく要求されないサービスの場合はｔがある程度以上大であれば有効とすると、認証情報の安全指標の変化に対し、対応した判定をすることができる。

第二の実施例

次に、認証手段が複数存在する例について図２を参照して説明する。

【0013】認証者装置１１では指紋入力部１２より、認証者の指紋情報ｅ１を生成出力し、更にパスワード入力部１４よりパスワードとして用いる４桁の数字ｅ２を生成出力し、チャレンジレスポンス部１５からチャレンジレスポンス認証における送信データｅ３を生成出力し、合計３種の認証情報を検証者装置２１に送るとする。送受信部２２で受信した認証情報ｅ１，ｅ２，ｅ３をそれぞれ指紋検証部23_1、パスワード検証部23_2、チャレンジレスポンス検証部23_3において検証処理を行い、それぞれｒ１＝ｈ１（ｅ１）、ｒ２＝ｈ２（ｅ２）、ｒ３＝ｈ３（ｅ３）なる検証結果（判定情報）を得る。ｈ２（・）は、４桁の数値が一致するかどうかを判定する関数とする。ｒ２は、０または１の値で、０ならばｅ２と不一致であり、１ならば一致とする。ｈ３（・）は、ｅ３と検証部23_3が導いたe_K（Ｒ）とを比較する関数とする。ｒ３は、０または１の値で、０ならば不一致であり、１ならば一致とする。チャレンジレスポンス認証では、まず検証部23_3が乱数Ｒを作成し、このＲを認証者装置１１に送る。認証者装

する。

【0008】

【課題を解決するための手段】この発明によれば監視信用機関を導入し、監視信用機関により、各種認証情報の安全性に関し監視を行うことにより、安全性に関する指標を検証者装置へ報告し、検証者装置は、認証者装置から認証に関する情報を受けたとき、前記安全性に関する指標を加味した検証結果を出力する。検証者装置へ与えられる認証情報が複数の場合は、それぞれの検証結果に対し、安全性の指標を加味し、その安全性指標が加味された検証結果を総合した検証結果を出力する。つまり認証者装置から検証者装置へあたえられる各種認証情報をｅ１，ｅ２，…＝ｅｉ（ｉ＝１，２，…）とし、それぞれの認証情報による判定情報（検証結果）をｒ１，ｒ２，…＝ｒｉ＝ｈｉ（ｅｉ）（ｉ＝１，２，…）とし、ここでｈｉ（・）は各種認証情報ｅｉに対する個別の判定関数（検証関数）であり、ｒｉは０～１の間の値である。総合的な判定結果ｔは、ｆ（r_{x1}，r_{x2}，…，s_{x1}，s_{x2}，…）＝ｔであり、ｘ１，ｘ２，…＝ｘｉ（ｘｉ∈１，２，…）は認証者と検証者の間で決められた検証結果ｒｉに関する選定を示すとともに、ｓ１，ｓ２，…＝ｓｉ（ｉ＝１，２，…）は監視信用機関から与えられた安全指標であり、ｆ（・・）は判定情報（検証結果）と安全指標を入力として、総合的な判定結果を出す関数である。なおr_0＝０、s_0＝０とする。検証者はこの結果ｔを入手し、これを用いて認証者の有効無効を判断する。

【0009】なお安全指標の決定については監視信用機関において、各認証方法について手法に応じて認証情報の安全指標を決定して、公表し、新しい認証方法が現われ認証情報の安全指標を決定し、また先に述べたように例えばＤＥＳ暗号を用いる認証方法において、その安全性が低下すると、対応する認証情報の安全指標を低い値に変更する。パスワードを用いる認証方法の場合は、利用者が認証手続を行うことを実施し始めた時に、利用者が監視信用機関３１にそのことを登録すると、監視信用機関はその登録から例えば１年ごとのように年数が経過するごとに、そのパスワードの認証情報に対する安全指標を低下させ、それを利用者に通知することも考えられる。

【0010】

【発明の実施の形態】以下図面を用いてこの発明の実施例について詳しく説明する。ネットワーク上での利用者認証を例とした場合で、認証者装置１１と検証者装置２１と監視信用機関３１とで構成され、これらは通信手段４１で互いに接続することが可能である。

第一の実施例

まず、認証手段が１つしか存在しない例、すなわち認証者と検証者の間にて選定がｘ１＝１，ｘ２＝ｘ３＝…＝０と定められた場合について説明する。

【0011】認証者装置１１は指紋入力部１２により認証情報として認証者の指紋情報ｅ１を生成して送信部１３にて検証者装置２１に送るとする。この場合、検証者装置２１は受信部２２で受信した指紋情報ｅ１を検証部（指紋検証部）23_1に入力して、ｈ１（ｅ１）＝ｒ１を演算して認証者の指紋に関する判定情報ｒ１を得る。ｈ１（・）は、受信指紋情報ｅ１と記憶部２４に記憶されている登録指紋との一致性を判定する関数とする。ｒ１は０～１の範囲の値で、０ならば検証者装置２１に登録されている認証者の指紋と離れていて、１ならば検証者装置２１の記憶部２４に登録されている認証者の指紋にきわめて近いとする。この検証結果ｒ１に対し、安全指標ｓ１を安全性加味部25_1で加味し、例えばｒ１ｓ１とする。この実施例では認証情報が１つしかない場合であるからｔ＝ｒ１ｓ１として判定結果が出力され、このｔを用いて認証者の認証可否を判断する。ｓ１は、監視信用機関３１から送られ、受信部２２で受信され、記憶部２４に記憶されている指紋に関する安全指標である。

【0012】このように検証結果に対し、安全指標ｓ１が加味されているため、検証者は、その判定結果ｔに応じて対処する、つまり例えば認証に合格するとあるサービスを行う場合、そのサービスによっては厳しく本人性が要求される場合はｔが十分大でなければ、無効とするが、それ程本人性が厳しく要求されないサービスの場合はｔがある程度以上大であれば有効とすると、認証情報の安全指標の変化に対し、対応した判定をすることができる。

第二の実施例

次に、認証手段が複数存在する例について図２を参照して説明する。

【0013】認証者装置１１では指紋入力部１２より、認証者の指紋情報ｅ１を生成出力し、更にパスワード入力部１４よりパスワードとして用いる４桁の数字ｅ２を生成出力し、チャレンジレスポンス部１５からチャレンジレスポンス認証における送信データｅ３を生成出力し、合計３種の認証情報を検証者装置２１に送るとする。送受信部２２で受信した認証情報ｅ１，ｅ２，ｅ３をそれぞれ指紋検証部23_1、パスワード検証部23_2、チャレンジレスポンス検証部23_3において検証処理を行い、それぞれｒ１＝ｈ１（ｅ１）、ｒ２＝ｈ２（ｅ２）、ｒ３＝ｈ３（ｅ３）なる検証結果（判定情報）を得る。ｈ２（・）は、４桁の数値が一致するかどうかを判定する関数とする。ｒ２は、０または１の値で、０ならばｅ２と不一致であり、１ならば一致とする。ｈ３（・）は、ｅ３と検証部23_3が導いたe_K（Ｒ）とを比較する関数とする。ｒ３は、０または１の値で、０ならば不一致であり、１ならば一致とする。チャレンジレスポンス認証では、まず検証部23_3が乱数Ｒを作成し、このＲを認証者装置１１に送る。認証者装

置11のチャレンジレスポンス部15はe_K（R）＝e3を計算する。Kは、認証者と検証者とが共有している鍵であり、e_K（・）は鍵Kによる暗号化関数である。認証者装置11はe3を検証者装置21に送る。検証部23_3は、送られてきたe3と自分が計算したe_K（R）とを比較し、一致すれば可、不一致ならば不可とする認証方法である。

【0014】各検証部23_1，23_2，23_3よりの検証結果（判定情報）r1，r2，r3に対し、安全性加味部25_1，25_2，25_3において安全指標s1，s2，s3がそれぞれ加味され、例えば、r1s1，r2s2，r3s3とされる。s1，s2，s3はそれぞれ、指紋、パスワード、チャレンジレスポンスに関する安全指標であり、監視信用機関31から送られ、送受信部22に受信され、記憶部29に記憶されたものである。これら安全指標が加味された検証結果に対し、それぞれ、総合判定結果tを正規化するために、任意に定めた重み付け係数w1，w2，w3が重み付け部26_1，26_2，26_3で掛算され、w1r1s1，w2r2s2，w3r3s3とされて総合判定部27に入力される。

【0015】総合判定部27ではここで例えば、t＝f（r1，r2，r3，s1，s2，s3）＝w1r1s1＋w2r2s2＋w3r3s3となる演算を行う。いま仮りに安全指標および重み付け係数を当初s1＝s2＝s3＝1，w1＝w2＝w3＝1／3であったとする。つまりこの例では安全指標s1，s2，s3の総和3で1を割り、各認証情報に対し均等な重み付け係数1／3とした場合である。このような重み付け係数を用いることにより、認証情報の数に拘わらず、同一尺度の総合判定値tを得ることができる。

【0016】所で時間の経過に伴い、4桁の数値によるパスワードは認証方法として不適であることが分かったとする。この場合、監視信用機関31はパスワードの安全指標s2を1からs2＝0．2と変更し、これを検証者装置21に伝える。このような安全指標の変更があった場合、第一の例として認証者が現状における認証の厳密さを維持したい場合は、重み補正部28でw1＝w2＝w3＝1／（s1＋s2＋s3）＝1／2．2なる補正演算を行って、新たにw1，w2，w3を1／2．2に定める。第二の例として認証者が認証の厳密さをより厳しくしたい場合は、w1，w2，w3を変更せずそのまま1／3とする。この場合は安全指標が小さくなったパスワードについては他の認証情報に対し相対的に重要度が低下されることになる。検証者装置21はこれらの値を関数fに代入して求めたtを用いて、認証者の認証可否を判断する。

【0017】重み付け係数w1，w2，w3としては、安全性の高い認証情報に対し大きく、例えば指紋にはw1＝0．5、パスワードにはw2＝0．1、チャレンジレスポンスにはw3＝0．4のように決ることもできる。何れの場合も判定結果tが0～1の値となるようにする。また認証者Aは指紋のみ、認証者Bはパスワードのみの認証情報を用いた場合を考える。この場合検証者装置21は、認証者Aの装置からの認証情報に対してはt＝w1r1s1を計算することでtを求め、認証者Bの装置からの認証情報に対してはt＝w2r2s2を計算することでtを求め、認証情報の種類にかかわらず検証者装置21の総合判定値tを同一尺度で判定することもできる。

【0018】検証結果r1，r2，r3に対し重み付け係数w1，w2，w3をそれぞれ乗算した後、安全指標s1，s2，s3を乗算してもよい。前記重み付け係数は必ずしも用いなくてもよい。またこの発明の認証方法は公衆通信網の通信を利用する場合に限らずイントラネットやLANのような局部的な通信網内の認証にも適用できる。従って、監視信用機関31は、この認証方法が適用される通信網ごとに設けられることになる。また検証者装置21は通常は主としてコンピュータによりプログラムを実行することによりその全体が機能される。

【0019】

【発明の効果】以上説明したように、この発明の第一の実施例によれば、監視信用機関が認証情報に対する安全指標を変更しこれを検証者装置に伝えることによって、検証者は時間の経過による認証手段の安全性低下に応じた検証結果を知ることができ、その認証を必要とする次の処理に要求される、例えば本人性の厳密さに応じて、判定結果tに対し可とするか不可とするかの判定をすることができる。

【0020】第二の実施例によれば、検証者装置が認証情報に対する安全指標を用いて総合的な判定結果を導くことによって、安全指標が時間により変化した場合に安全指標が低下した認証情報に対する検証結果に対する考慮が低下され、認証方法を変更することなく、総合判定結果tの安全性は安全指標の低下前と実質的に同様に保持される。また複数の認証者が同一の認証手段を持たない場合においても、検証者装置は複数の認証者装置からの異なる種類の認証情報に対し、同一の基準に基づいて認証の正否を判断できる。

【図面の簡単な説明】

【図1】この発明の第一の実施例の方法が適用されるシステムの機能構成例を示す図。

【図2】この発明の第二の実施例の方法が適用されるシステムの機能構成例を示す図。

【図3】従来の認証方法を説明するための図。

【図1】

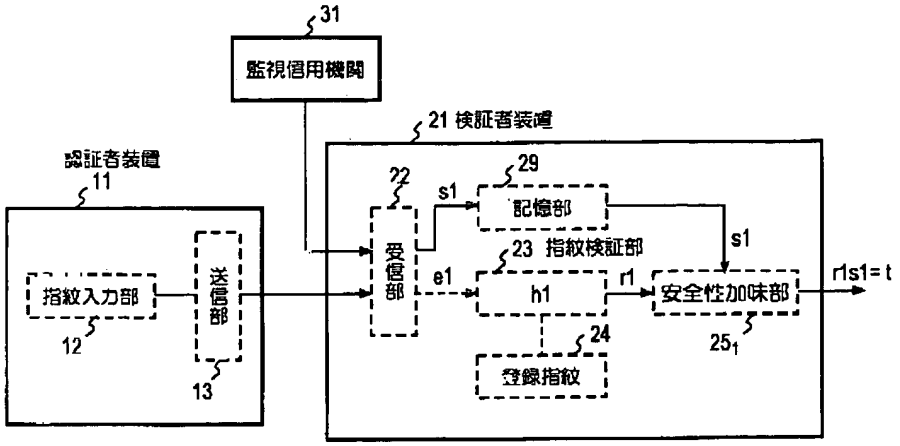


図1

【図2】

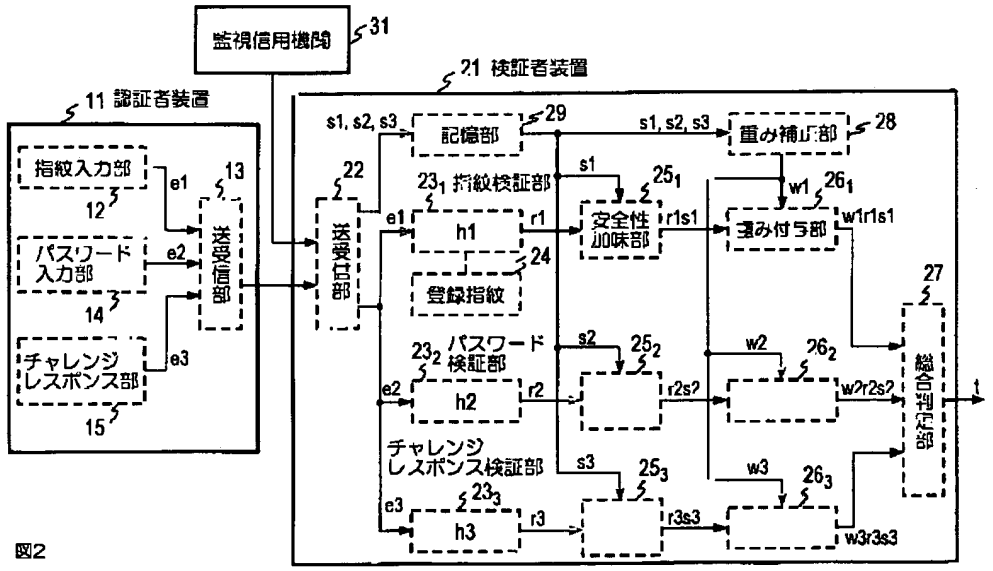


図2

【図3】

図3

フロントページの続き

(72)発明者　郷原　純一
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

Ｆターム(参考)　5B085 AE01 AE06 AE23 AE25 AE29
5J104 AA07 KA01 KA17 MA01 NA02
PA07